Appendix 1 – Domain Technical Reference Models

1.0 General

This document classifies and describes technologies for each of the seven domains identified by California's Technical Architecture Framework (TAF) (see figure 1). A technical reference model (TRM) is provided for each of these domains along with detailed descriptions of disciplines and technology areas contained therein. This information is intended to provide a common understanding of technology groupings and technology components across all state agencies and departments from which Enterprise Technical Architectures (ETA) can be developed. Product Components are not included as they will be determined by domain teams during the ETA development process.

Domain TRM disciplines and technology areas will change over time. State level domain teams (once formed) will maintain these TRMs by conducting periodical reviews or responding to Agency/Departmental change requests. While using a domain TRM to create an organization's ETA, questions may arise when a product component (technology or standard) currently in use does not appear to be included in one of the existing technology areas. This could mean it is either an emerging or an obsolete technology. Please contact CEAP Office (916) 739-7637 for assistance.

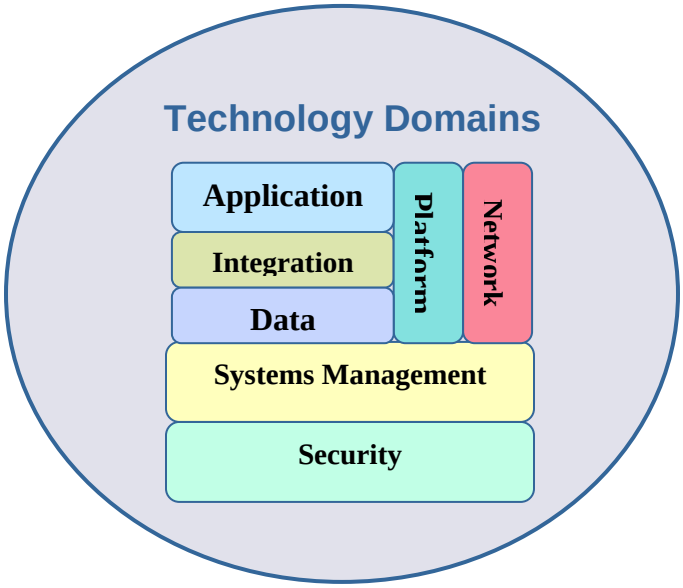

Figure 1 California's Technology Domains

2.0 Application Domain TRM

The Application Domain TRM that lists and describes the disciplines and technology areas included in this domain is as follows (Table 1):

Application Domain TRM	
Disciplines	**Technology Areas**
Access Channels - the means used to provide the interface between an application and its users.	**Terminals -** a small physical structure usually including a computer and a display screen that typically allows user login to an application and displays information.
	Windows Applications - provides access to applications using Microsoft Windows.
	Web Browsers - the program that serves as a front end to the World Wide Web and web enabled applications. Allows enter of Uniform Resource Locator (URL) address in order to view a website and interprets hypertext link to activate communications with and access to an application.
	Wireless/PDA - defines the technologies that use transmission via the airwaves. Personal digital assistant (PDA) is a handheld computer that serves as an organizer for personal information (e.g. Blackberry, cell phone, etc.)
	Collaboration Communications - allows exchange of computer generated and stored messages by telecommunications (email) or a small physical device that displays information to people walking by (i. e. Kiosk)
	Other Electronic Channels - defines other media of information exchange and interface between a user and an application e.g. Appl. to Appl., Web Services, URL, IVR)
Presentation – means by which information and data from an application is presented to or received from the user.	**Static/Dynamic Display –** consists of the software protocols used in a web context that are either used to create a pre-defined, unchanging graphical interface between the user or the software used to allow changes to an interface while the program is running.
	Server Side – consists of the software protocols and constructs used to generate and provide the data needed for content rendering in support of the graphical interface between the user and the software (e.g. JSP/Servlet, ASP/ASP.NET, PHP, etc).
	Content Rendering - defines the software and protocols used to transform data for presentation in a graphical user interface (e.g. HTML, DHTML, XHTML, CSS, etc.).
	Wireless/Mobile/Voice - consists of the software and protocols used for wireless and voice-enabled presentation devices (e.g. WML, XHTML Mobile Profile, & Voice XML).
	Display Terminal - software and protocols used for terminal emulation to present data to or accept data from the user (i.e. 3270, 5250).
	Other – consists of the software and protocols needed to transmit a small amount of information to and from the server in order to give the user the most responsive feedback or the software needed to support the user interface as part of speech-enabled or Interactive Voice Response (IVR) applications. (e.g. Ajax, Computer Supported Telecommunications Applications (CSTA), Speech Application Language Tag (SALT) etc).

Application Domain TRM	
Disciplines	**Technology Areas**
Business Component – part of the application that defines and implements the business functionality of an application, includes logic, orchestration of business processes, and/or a set of business components.	**Business Logic -** defines the software, protocol or method in which business rules are enforced within applications. The software language used may be either platform dependent (.NET/MF) or independent (J2EE).
	Business Rules - defines the set of parameters or constraints that the business activities must comply.
	Workflow – is based on either a document workflow or a detailed business process flow. Both implement a series of tasks within an organization to produce a final outcome. Technology ensures that at each stage in the workflow, one individual or group is responsible for a specific task and that once the task is complete, the work is passed to the individual(s) responsible for the next task. These people are notified and receive the data needed to execute their stage of the process.
	Process Flow – uses web services and provides an environment for the process flow to take place. Web services typically use BPEL and terminal environments consist of those supported by mainframe, Unix, or Windows.
	Transaction - a type of processing in which the computer responds immediately to user requests. Each request is considered to be a transaction (e.g. CICS, Tuxedo, etc.).
	Data Connectivity - means by which the application interacts with the database within the context of the application (e.g. JDBC, ODBC, ADO, OLE/DB, Data Access Objects, DB Connectors, etc.).
Shared Applications and Services – applications and services jointly managed or used by two or more agencies or departments. Includes both Commercial-Off-the-Shelf (COTS) software products and software collaboratively developed within the enterprise or specific community of interest.	**ERP –** consists of a multi-module software system that supports enterprise resource planning. Uses an integrated set of technologies including database, integration (middleware & interoperability), portal, and software development tools to provide applications for managing HR/Payroll, Finance, Procurement, CRM, etc.
	Portal - common or federated set of websites that offer a broad array of user resources and services, such as search engines, and on-line payments, licensing, registration, etc.
	GIS - includes a specialized set of technologies required to implement a graphic information system (GIS). Provides a common way to store, retrieve, and display contextual views of geospatial information.
	Collaboration - software designed for groups to facilitate communication and workflow, including email, videoconferencing, workflow, chat, and collaborative editing systems. Specific classes of technology include email, calendaring, computer supported meeting (or Learning) environments, newsgroups, videophones, or chat.
	Enterprise Content Management – a common set of technologies, tools, and methods used to capture, manage, store, preserve, and deliver information, content, and documents related to organizational processes..
	Payment Service - software that functions to provide a common payment service based on a set of standards and business related access and conventions.
	Other Shared Services – additional developed software that functions to provide a common service (other than payment) based on a set of standards and business related access and conventions.

Application Domain TRM	
Disciplines	**Technology Areas**
	(e.g. licensing, identity, etc.)
Software Engineering - covers both the technical aspects of building software systems and related management issues, such as SCM and testing.	**Modeling (UML & CASE Mgmt)** - the process of representing entities, data, business logic, and capabilities for aiding in software engineering. These technologies usually include UML & CASE Management components.
	Integrated Development Environment (IDE) – consists of the hardware, software and supporting services that facilitate the development of software applications and systems. Typically provides a GUI builder, a text or code editor, a compiler and/or interpreter and a debugger (e.g. Visual Studio, Delphi, JBuilder, FrontPage and DreamWeaver are all examples of IDEs).
	Other Development Environments – comprised of development environments, not IDE, provided for mainframes (e.g. COBOL/IMS, Natural/Adabas, CICS)
	Software Configuration Management (SCM) - applicable to all aspects of software development and focuses on the control of all work products and artifacts generated during the development process. Supports SCM functions including Requirements Management & Traceability as well as Version Control, Defect, Issue, Task, Change, and Deployment Management.
	Test Management – supports consolidation of all test management activities and results including test planning, design (test scenarios & test cases), execution, reporting, and retesting.
Process Control Management – supports processes needed to manage both individual projects and the collective set of the applications and IT services being maintained by the enterprise.	**Project Management–** tools that support implementation of a standardized project management methodology used for software development projects. Includes best practices as well as templates and reports needed for project phases including origination, initiation, planning, execution & control, and closeout phases.
	Portfolio Management – tools used to provide a structured approach to categorize, evaluate, prioritize, and manage an organization's technology assets including applications, computer services, and hardware infrastructure.

Table 1 – Application Domain TRM

3.0 Data Domain TRM

The Data Domain TRM that lists and describes the disciplines and technology areas included in this domain is provided below (Table 2):

Data Domain TRM	
Disciplines	**Technology Areas**
Data Management – is the management of all data/information in an organization. It includes data standards and data administration for defining data and the way in which people perceive and use it.	**Data Standards -** used to describe how, when and by whom a particular set of data is collected, and how the data is formatted prior to implementation in a DBMS (e.g. Meta Data, XML Schemas, etc.)
	Data Administration – provides collective control and management of all information used within the enterprise. Maintains functional requirements, logical design, standards, and a data dictionary system to guide development of all data bases.
	Backup/Restoral – utilities that provide the means to backup or restore an entire data base or portion thereof.
Database – refers to a collection of information organized in such a way that a computer program can quickly select desired pieces of data.	**Data Modeling –** supports the analysis of data objects and their relationships to other data objects. Supports progression from a conceptual data model to a logical model (schema) to physical implementation within a DBMS.
	Operational Data Store – includes database management systems (DBMS) that provide management, administration, performance tuning, and analysis tools for data bases (e.g. DB2, Oracle, Natural/ Adabas, OLTP, etc.)
	Geospatial – the specialized set of technologies required to implement storage retrieval, and display contextual views of geospatial information. Implements GIS mapping and imaging repositories.
Information – consist of the tools, languages and protocols used to extract data from a data store and process it into useful information or exchange data between different databases.	**Data Warehouse (& Data Marts) –** supports the combining of many different databases across an entire enterprise. Components include tools and/or developed systems that extract data from other systems, transform, and load the data to the warehouse and then present a coherent picture of the business conditions at a single point in time. Supports Business Intelligence reporting and trend analysis. Enterprise data warehouses that are sub divided into smaller logical units to support specific workgroups are called data marts.
	Extraction Transformation & Load (ETL) - used to migrate data from one database to another, to form data marts (or data warehouse) and implements conversion from one database format or type to another e.g. Informatica, etc.)
	Data Analytics - provides the means to study existing groups of data to discover hidden patterns that can be used to predict future behavior (e.g. Data Mining, OLAP, BI, etc.).
	Reporting - consists of tools that take the results of predefined or ad hoc queries and tailor the data for output.

Table 2- Data Domain TRM

4.0 The Integration Domain TRM

The Integration Domain TRM outlining the disciplines and technology areas included in this domain is provided below (Table 3).

Integration Domain TRM	
Disciplines	**Technology Areas**
Interface – defines the capabilities of communicating, transporting and exchanging information through a common dialog or method.	**Service Discovery –**defines the method in which applications, systems, or web services are registered and discovered.
	Service Description – defines the method for publishing the way in which web services or applications can be used.
	Middleware – increases flexibility, interoperability, and portability of existing infrastructure by linking or "gluing" two otherwise separate applications (e.g. Enterprise Application Integration, Messaging, Enterprise Service Bus, Screen Scraping, & other).
	Legacy – includes transactional, messaging, terminals, & batch interfaces typically used for interacting with older mainframe based systems.
Interoperability – defines the capabilities of discovering and sharing data across disparate systems and vendor platforms	**Data Format/ Classification –** defines the structure of a file. There are hundreds of formats, and every application has many different variations (database, word processing, graphics, executable program, etc.). Each format defines its own layout of the data. The file format for text is the simplest.
	eXtensible Markup Language (XML) – standard format for web data, and is beginning to be used as a common data format at all levels of the architecture. Includes the many specialized vocabularies of XML being developed to support specific Government and Industry functions.
	Data Transformation –consists of the protocols and languages that change the presentation of data within a graphical user interface or application.

Table 3 –Integration Domain TRM

5.0 The Platform Domain TRM

The Platform Domain TRM outlining the disciplines and technology areas included in this domain is provided below (Table 4).

Platform Domain TRM	
Disciplines	**Technology Areas**
Hardware Platforms –	**Mainframe –** a very large computer capable of supporting hundreds or even thousands of users simultaneously by managing LPARs.
	Mid-range Computer – a powerful workstation or mini-computer that uses the UNIX operating system to provide the computing environment and can support multiple users.
	Personal Computing - a small desktop, laptop, or handheld computer that is typically provided for the exclusive use of one person. Can be based on Windows, Mac, laptops, or PDA's.
	Embedded/Appliance – a computer device consisting of both hardware and software that performs a specific function as part of a larger system (e.g. the computer that controls the automotive systems within a vehicle or the computer that manages a security monitoring system).
	Virtual Server – software used to partition a single server platform (excluding mainframe) so that it appears as multiple servers. Takes advantage of unused CPU capacity to increase service availability and performance (e.g. VMware, Xen, Microsoft Virtual Server, User-mode Linux, Linux-Vserver, Free VPS, OpenVZ, and, HP Virtual Server).
	Operating System - the main control program of a computer that schedules tasks, manages storage, and handles communication with peripherals. Presents a basic user interface (e.g. desktop) when no applications are open. Provides a software platform on which other programs can run (e.g. Windows, ZOS, MVS, UNIX (i.e. Solaris, RISC, HPUX, AIX, & Linux)).
Functional Servers – are computers on a network that manage network resources and share applications for multiple users. Includes the hardware, operating system, server software, and networking protocols.	**Web Server –** a computer that provides World Wide Web services on the Internet. Includes the hardware and operating system, web server software, TCP/IP protocols, and the Web site content (Web Pages). If the Web server is used internally and not by the public, it may be known as an "intranet server".
	Media Server – used to provide optimal management of media-based files such as audio and video streams and digital images.
	Mail Server - moves and stores mail over the organization's networks via LANs and WANs and across the Internet.
	Application Server – provides support for the business logic component in a three-tiered environment and acts as middleware to connect database information (which is usually coming from a database server) and the end-user or client program (that is often running in a Web browser).

Platform Domain TRM	
Disciplines	**Technology Areas**
	File Server – moves one or more files securely between computers while providing file security and organization as well as transfer control (e.g. FTP).
	Database Server – provide DBMS services and contain the data for applications.
Supporting Platforms – the underlying hardware and software for a system which defines a standard around which a system can be developed. Defines the physical devices, facilities, and standard technologies that provide the computing environment.	**Wireless/Mobile** – defines the operating system, programming languages, and protocols used to support resourced constrained devices including digital mobile phones, pagers, personal digital assistants and other wireless devices (e.g. WAP, JME).
	Platform Independent - defines the operating systems and programming languages that are able to execute and run on multiple platforms (i.e. Java) or operating system. A platform is the underlying hardware and software comprising a system (e.g. J2EE).
	Platform Dependent - defines the operating system and programming languages that are able to execute and run on a specific platform or operating system. A platform is the underlying hardware and software comprising a system (e.g. Windows & .NET).
	Portal Infrastructure – provides focus points for interaction by providing integration and single-source access to enterprise information.
Peripherals – computer devices that are not part of the essential computer or network. They can be external or internal and can be for a PC, workstation, or network.	**Printers -** devices that print text and/or graphics on paper.
	Scanners/Faxes - imaging devices, OCR, bar code scanners, faxes.
	Other – includes cameras, video, and external storage devices.
Storage Systems – storage platforms are designed to provide shared storage access across a network.	**Storage Area Network (SAN) –** a high-speed network that connects multiple storage devices so that they may be accessed on all servers in a Local Area Network (LAN) or Wide Area Network (WAN) or by the mainframe.
	Network Attached Storage (NAS) - is a server that is dedicated to nothing more than file sharing. Consists of a disk or multi-disk system (i.e. RAID) for storing data files, and the software needed for configuring and mapping file locations to the network-attached device. The device is attached to a LAN with its own network address and file requests are mapped by the main server to the NAS server.
	Tape – technologies used to store data on magnetic media. Usually involves tape drives and heads used to mount tapes so that they can be read, written to, or erased..
	Other Storage Media – involves various storage media and devices including flash memory (e.g. memory sticks, USB Keys), disk storage (e.g. optical, hard disk, removable magnetic media (floppy or zip)), and magnetic bubble memory. Also includes hierarchal storage management (HSM) systems that implement policy-based storage

Platform Domain TRM	
Disciplines	**Technology Areas**
	management to provide transparent, economical file retrieval from backup or archive storage media.

Table 4 – Platform Domain TRM

6.0 The Network Domain TRM

The Network Domain TRM outlining the disciplines and technology areas included in this domain is provided below (Table 5).

Network Domain TRM	
Disciplines	**Technology Areas**
Internet/Extranet –.a networking infrastructure that connects networks to networks globally forming a network in which any computer can communicate with any other computer as long as they are both connected to the Internet. Extranet refers to a network that is only partially accessible to those on the internet. Access is provided for various levels of accessibility to outsiders based on network security.	**Wide Area Network (WAN) –** interconnects computers and devices over a wide geographic area using telephone lines, fiber optic cables, protocols, and satellite communications. Typically created by using gateways and routers to connect geographically separate LANs. Uses standard protocols for synchronous communication of digital information packets over optical fiber (e.g. frame relay, ATM, OSPF, fiber optic, T1, T3, IP, IPv6, SONET/SDH, STS, and OC).
	Metropolitan Area Network (MAN) - a data network architecture and infrastructure designed for a town, city, or school campus.
Intranet – similar to an internet (e.g. network based on TCP/IP protocols) but belongs to an organization and is accessible only to the organization's employees, or others with authorization An intranet's Web sites look and act just like any other Web sites, but there is a firewall that fends off unauthorized access.	**Local Area Network (LAN) –**interconnects devices over a geographically small area, typically in one building or part of a building. Provides protocols that allow the sharing of resources and the exchange of data (e.g. Ethernet, TCP, etc.)
	LAN Connectivity - provides backbone for LANs and remote access. Includes hubs, switches, NICs, VPN, and remote desktops.
	Network Operating System (NOS) – adds network features to a basic operating system that includes special functions for connecting computers and devices on a LAN (e.g. Novell Netware, Microsoft Windows Server, etc.).
Wireless - networks that are connected by radio media rather than by wires. Can be used for voice, data, video, and images and can be interconnected with regular computer networks. Includes packet, radio, spread spectrum, cellular technology, satellites, and microwave.	**Wireless Protocol/Transport -** a set of open, global specifications that allows digital mobile phones, pagers, personal digital assistants and other wireless devices to securely access and interact with Internet/intranet/extranet content, applications, and services (e.g. WAP, CDSM, GSM, Bluetooth, 802.11a/b/g, etc.).
	Wireless Services – includes the services that can be provided to hand held devices such as cell phones, and PDAs (e.g. eMail, other)
	Wireless Fidelity (WiFi) - refers to an over-the-air connection with a wireless client and a base station or between two wireless clients. Synonymous with IEEE802.llb.
Network Appliances – specialized devices used to control access to and/or pass data between networks.	**Firewalls -** used to prevent unauthorized internet users from accessing private networks (i.e. intranets and extranets) connected to the Internet. Insures all messages entering or leaving the intranet pass through the firewall first.

Network Domain TRM	
Disciplines	**Technology Areas**
	Proxy/Reverse Proxy Servers – sits between client and network server and is used to filter requests. Provides access to files by retrieving them either from its local cache or from the remote server. Can be used to prevent access to a specific set of web sites.
	Gateway - is a node on a network that serves as an entrance to another network (e.g. allows LAN to connect to a WAN). Uses a computer to route the traffic from a client workstation to the outside network that is serving the web pages. Often acts as a proxy server and firewall as well.
	Router – is a specialized computer that stores and forwards data packets between networks based on , possible paths to the destination address and picking the best route based on traffic load and number of hops.
Network Services – provides special network functions that allow access or connectivity to network resources or devices.	**Directory Services -** identifies all network resources, including email addresses, computers, and peripheral devices such as printers, and makes them accessible to users and applications (e.g. AD, LDAP, X.500, WINS, etc.)
	Dynamic Host Configuration Protocol (DHCP) – used for assigning dynamic IP addresses to devices on a network.
	Domain Name Server (DNS) - an Internet service that translates domain names into IP addresses.
	Network Management – supports LAN or WAN maintenance and operational activities by monitoring network performance (e.g. throughput, component failure, Network Alerts, etc.) and security (Digital Encryption, IP Security, Spam Blocking).
	Voice/IP – is the routing of voice conversations over the Internet or through any other IP-based network.

Table 5 Network Domain TRM

7.0 Systems Management Domain TRM

The Systems Management Domain TRM outlining the disciplines and technology areas included in this domain is provided below (Table 6).

Systems Management Domain TRM	
Disciplines	**Technology Areas**
Service Support – focuses on supporting the users who are having difficulties or are requesting a change to an IT service and ensuring their access to the appropriate services needed to carry out their business functions.	**Service Desk** – provides central point of contact (e.g. Help Desk, Call Center, Contact Center, etc.) for the customers to report their service problems, and for the IT organization to record contact and resolution information. If request is not met by service, then it supports creation of an incident and initiates a chain of processes (i.e. Incident Management, Problem Management, Change Management, Release Management and Configuration Management to achieve resolution.
	Incident Management – manages any event reported to the service desk which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service. Assigns ownership, monitors and tracks resolution, and provides communication for those involved.
	Problem Management – attempts to minimize the adverse impact of incidents and problems on business that are caused by errors within the IT infrastructure and to prevent recurrence of incidents related to these errors. Often identified as a result of multiple Incidents that exhibit common symptoms for which workarounds are developed until the root cause of the problem can be corrected. Supports trend analysis, targeted support actions, and provides information.
	Change Management - ensures that standardized methods and procedures are used for efficient and prompt handling of all changes to controlled IT infrastructure, in order to minimize the number and impact of any related incidents upon service.
	Configuration Management – tracks all individual Configuration Items (CI) in a system which may be as simple as a single server, or as complex as the entire IT department. Supports creation of parts lists for every CI (hardware or software) in the system, defining the relationship of CIs in the system, tracking the status of each CI, tracking all requests for system changes, and verifying the CI parts list.
	Release Management - provides platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure. Implements planned roll out of SW and a process to guarantee SW will function correctly and effectively on available HW.
Service Delivery - concerned with sustaining current service performance	
	Service Level Management - provides continual identification, monitoring, and review IT services specified in

Systems Management Domain TRM	
Disciplines	**Technology Areas**
levels and addressing future needs of IT services for the business as a whole.	service level agreements in conjunction with the operational processes to control their activities. Allows service administrators to monitor the performance or assess the impact of changes to a system based service agreements.
	Capacity Management - supports the optimum and cost effective provision of IT services by matching projected IT resource requirements to the business trends. Determines when minimum performance requirements can no longer be met and identifies the technology specifications needed for required upgrades.
	Availability Management - allows organizations to maintain the highest level of IT service availability at a justifiable cost in order to support the business.
	(IT) Financial Management - provides support for implementation of cost-effective management of the IT assets (e.g. HW, SW packages, & SW licenses) and resources used in providing IT services. Includes lifecycle management of all IT assets from procurement through disposal. Allows monitoring of outsourced services by attributing costs of the services delivered to the organization's customers and provides business cases for supporting proposed service changes.
	Continuity Management – facilitates management, implementation, and monitoring of the disaster recovery plans to insure rapid restoration of data center or network IT services in the event of a disaster.
	Security Management – helps document and manage security requirements dictated by the clients and other mandates. Supports translation of requirements into security services and security service quality for inclusion in Service Level Agreements.

Table 6 Systems Management Domain TRM

8.0 The Security Domain TRM

The domain taxonomy outlining the disciplines and technology areas included in the Security Domain is provided below (Table 7):

Security Domain TRM	
Disciplines	**Technology Areas**
Administration & Management – furnishes the techniques for insuring that information stored on a computer or network cannot be accessed or compromised by any individuals without proper authorization.	**Access Policy**. – outlines a set of rules based on legal mandates and determines how policies are enforced to govern data access, computer/network usage, password handling, encryption, email, attachments, and more. Specifies role-based rules for individuals or groups and identifies IT Administrator exceptions. Lays the framework for internal computer-network security practices and for external interaction with other networks (i.e. the Internet).
	Electronic Signature – electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record. Includes digital signature protocols and cryptographic techniques, either on a document, or on a lower-level data structure to validate an action or directive.
	Security Monitoring & Alerts – allows security administrators to monitor the interaction of the organization's network with other networks (i.e. the Internet). Uses a variety of tools to prevent unauthorized access to the network and to detect, alert, and respond to malicious attacks or attempts to penetrate network security.
	Virus Protection - means used to protect a network or a computer from computer viruses. Involves maintaining a repository of information about viruses and anti-viruses and distributes patches/downloads needed to avoid contamination.
	Compliance/Audits – provides the means by which policies are enforced and the wherewithal to audit computer and network usage using various activity logs to determine policy effectiveness or research incidents of non-compliance.
	Forensic Analysis - includes the tools (e.g. Autopsy, Encase, etc.) to conduct investigations into computer related incidents, whether the incident is an external intrusion into your system, internal fraud, or staff breaching your security policy. Supports correlation analysis as well as other investigative techniques.
	Data Encryption – encryption needed to secure the data contained on personal computers (e.g. PCs, laptops, PDAs, etc.) and portable storage media (e.g. floppy disks, flash/memory sticks, CD's, etc.) or needed to provide secure remote access (e.g. SSL, Tumbleweed, etc.)
Identity Management - manages the unique names of persons, devices, or the combination of both that is recognized by a system. Furnishes authentication, authorization, and	**Identity Policy** – outlines those rules needed for defining and passing identity information (i.e. assertions and certificates) as well as the rules needed for authenticating identities.
	Trust Relationships – the framework for establishing

Security Domain TRM	
Disciplines	**Technology Areas**
accounting services based on receipt of valid identity data to ensure the security of networks and resources.	trusted relationships, and management of token processing protocols (e.g. STS).
	(Federated) Identity Standards – includes the protocols and standards developed to support identity management, authentication, and access control (e.g. OASIS (WS-Federation & SAML), Liberty Alliance, etc.).
Privacy - ability of an individual or group to keep their lives and personal affairs out of public view, or to control the flow of information about them as directed by legal mandates or user preferences.	**Compliance Management Policy –** provides a framework for defining and meeting privacy requirements needed to meet legal mandates and other privacy policy requirements (e.g. WS-Privacy).
	Profiling - defines roles, standards, audits, and tools that implement profile management (i.e. controls for establishing, maintaining, and utilizing privacy profiles).
	Personalization – software/tools that allow the user to determine what information to share with others in terms of personal preferences and permissions.
Web Services Security – frameworks and standards established for implementing secure access to and proper handling of data passed across the Internet and other networks (e.g. WS*) Insures message integrity and confidentiality.	**Web Service Standards** - standards used for implementing web service security (e.g. WS-Security, WS-Secure Conversation, WS-Privacy, WS-Policy, WS-Authorization, XML Signature).
	Security Architectures –vendor tool sets that are used to implement security standards and approaches (e.g. from OASIS and/or Liberty Alliance). Includes specific standards, formats, protocols, and procedures Microsoft WSE/WCF, IBM, etc.).
	Infrastructure – technologies used for identifying and exchanging messages between multiple end points based primarily on SOAP messaging (e.g. SOAP, XML, WS-Addressing, WS-Routing, & WS-Reliability)
	Encryption - translation of data into a secret code to achieve data security. Requires a key to encrypt data and a secret key or password to decrypt data into plain text. Keys can use asymmetric encryption (public key encryption) or symmetric encryption. (e.g. (PKI, secure socket layer, XML Encryption, & certificates).

Table 7 Draft Security Domain TRM